Force Protection

Air Force Doctrine Document 2–4.1

29 October 1999

This document complements related discussion found in Joint Publications 3-07, *Joint Doctrine for Military Operations Other Than War;* JP 3-10, *Joint Doctrine for Rear Area Operations;* and JP 3-11, *Joint Doctrine for NBC Defense.*

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
29/10/1999	N/A	-

Title and Subtitle Force Protection Air Force Doctrine Document 2-4.1	**Contract Number**
	Grant Number
	Program Element Number
Author(s)	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Secretary of the Air Force Washington, DC	**Performing Organization Report Number**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms	
Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** SAR
Number of Pages 50	

BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE DOCTRINE DOCUMENT 2–4.1
29 October 1999

OPR: HQ AFDC/DR (Lt Col Robert W. Christensen)
Certified by: HQ AFDC/DR (Col Thomas A. Bowermeister)
Pages: 46
Distribution: F
Approved by: TIMOTHY A. KINNAN, Major General, USAF
Commander, Headquarters Air Force Doctrine Center

FOREWORD

Increases in the lethality of international and domestic threats dictate that the Air Force must take strong measures to protect our personnel and installations, at home and deployed. How the Air Force protects its forces is critical to global engagement. An aerospace expeditionary force (AEF) that is poised to respond to global taskings within hours reasonably expects its forces to be protected.

Commanders at all levels must have an effective force protection program. Commanders are responsible for protecting their people and the war-fighting resources necessary to perform any military operation. We are obligated by our past, present, and future to ensure force protection is a part of Air Force culture.

The Air Force must continue to develop and refine doctrine that promotes the most effective way to achieve force protection. Understanding and utilizing this doctrine are the paths to successful protection of our people and resources.

TIMOTHY A. KINNAN
Major General, USAF
Commander, Air Force Doctrine Center

29 October 1999

TABLE OF CONTENTS

INTRODUCTION

PURPOSE

This Air Force Doctrine Document (AFDD) establishes doctrinal guidance for organizing and employing force protection capabilities at the operational level across the full range of military operations. It is a critical element of US Air Force operational-level doctrine and as such should form the basis from which Air Force commanders plan and execute their force protection mission. This AFDD implements Air Force Policy Directive (AFPD) 10-13, *Air and Space Doctrine*.

APPLICATION

This AFDD applies to all Air Force military and civilian personnel (includes AFRC and ANG units and members). The doctrine in this document is authoritative but not directive. Therefore, commanders need to consider not only the contents of this AFDD, but also the particular situation when accomplishing their missions.

SCOPE

Air Force assets (people, weapons, information, and support systems) can be used across the range of military operations at the strategic, operational, and tactical levels of war. This AFDD discusses the fundamentals of organization and employment of Air Force force protection capabilities required to support the operational missions assigned to commanders in chief (CINCs) and carried out by air component commanders.

CHAPTER ONE

FORCE PROTECTION OVERVIEW

> ***Every airfield should be a stronghold of fighting air groundmen, and not the abode of uniformed civilians in the prime of life protected by detachments of soldiers.***
>
> **Winston Churchill**
> **29 June 1941**

The post-Cold War period is characterized by a significant shift in the Air Force functions and an increased exposure of its resources to the worldwide enemy threat. Today, potential opponents are more unpredictable and US assets are more at risk to enemy attack. Additionally, there is an increase in the availability of high and low technology weapons and weapons of mass destruction (WMD). US aerospace power requires protection from these threats at home station and abroad.

FORCE PROTECTION DEFINED

Force protection is everyone's job.

Force protection **(FP) is a collection of activities that prevents or mitigates successful hostile actions against Air Force people and resources when they are not directly engaged with the enemy.** A successful hostile action is one that, if executed, would directly or indirectly threaten our ability to accomplish the combatant commander's mission. Such hostile actions may include environmental, health, and safety threats.

FP is accomplished by a security program designed to protect service members, civilian employees, family members, facilities, and equipment in all locations and situ-

ations. This is accomplished through planned and integrated application of the following: combatting terrorism, physical security, operations security, and personal protective services. FP is supported by intelligence, counterintelligence, and other security programs.

FP measures are layered to be defensive (passive and active) or offensive, and each should **include an awareness of the actions of every element of a combat force.**

Defensive Force Protection

Passive Force Protection

Hardened aircraft shelters provide passive force protection for vital Air Force resources.

Passive force protection (PFP) measures **negate or reduce the effects of hostile acts or environmental and health threats on *Air Force assets* by making them more survivable.** This can be **proactively accomplished** through training, education, hardening, camouflage, concealment, deception, information security, and operations security. Some examples of PFP are hardened facilities, immunizations against biological agents, comprehensive individual fitness programs, predawn AEF deployment, and movement of family members onto the base during emergencies.

Active Force Protection

Active force protection (AFP) measures **provide a defense against a perceived or actual threat and,** if necessary**, serve to deny, defeat, or destroy hostile forces** in the act of targeting *Air Force assets.* Some examples include: enhanced owner/user work area security; executing countersurveillance operations; surveillance of vulnerability points; and defeating a hostile force in a firefight at the perimeter.

Offensive Force Protection

Offensive force protection (OFP) is **preemptive measures taken to deny, defeat, or destroy hostile forces before they are committed to**

direct hostile activity but whose intent is to target *Air Force assets* when they are not engaged in combat operations. Some examples are detecting, capturing, and detaining known terrorists and shunning network hackers prior to their affecting computer networks.

> ***I expect that our combat battalions will be used primarily to go after the VC [Viet Cong] and that we will not be forced to expend our capabilities simply to protect ourselves....Therefore, ...all forces of whatever service who find themselves operating without infantry protection ...will be organized, trained, and exercised to perform the defense and security functions.***
>
> **General William C. Westmoreland, 1965**

FORCE PROTECTION FUNDAMENTALS

The following is what airmen should know.

- ***Force protection is critically important.*** It is **each commander's** and **individual's responsibility.**
- Force protection means the Air Force can **execute its mission with increased freedom and reduced fear in an era of heightened threats.**
- Force protection **does not mean the Air Force will be free from attack; it assumes enemy action and threatening conditions.**
- Force protection represents the Air Force's best methods for dealing with the potential for attack, and it **preserves freedom of action.**
- Force protection does not apply to aerial combatants engaged with an enemy in combat air operations**. If you are not directly engaged in combat air operations against the enemy, you are engaged in force protection.**
- Force protection is built on the concept of full-dimensional protection. It provides **multilayered protection of forces and facilities** at all levels.

✪ Force protection requires a collaborative, integrated, cross-functional effort. Members of civil engineers, security forces, medical, communications, explosive ordnance disposal, intelligence, and counterintelligence communities all play key roles in force protection.

Defense of air bases against ground attack has been traditionally viewed within the USAF as a Security Police problem….it is more properly viewed as an airpower problem because airpower is so critical to US national military strategy and the US way of war.

David Shlapak and Alan Vick,
Check Six Begins on the Ground

FORCE PROTECTION CONSTRUCTIVE MODEL

Intelligence, risk-based assessments, countermeasures, and awareness underpin every FP effort. These, coupled with **command and control,** result in a constructive model for FP. The constructive model in figure 1.1 outlines the relationships among these areas of FP. This constructive model adequately describes the elements of FP. However, to be effective they should be integrated in the overall FP operational effort.

Intelligence

Effective intelligence is critical to determining the threats to the force. Identifying a threat strengthens the overall force protection effort. FP intelligence and counterintelligence personnel should be capable of ana-

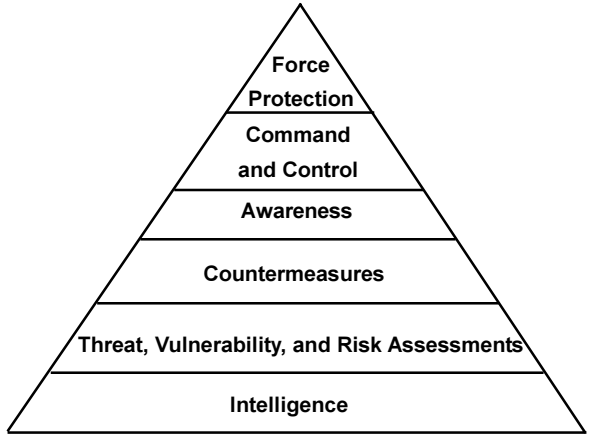

Figure 1.1. Force Protection Constructive Model

lyzing a broad range of threats. These threats may be conventional military units, special forces, terrorist groups, riotous civil populations, environmental and health hazards, chemical or biological agents, radioactive material, cyberterrorists, criminal elements, religious zealots, extremist groups, and the weapons any of these groups might select. With this extremely wide variety of threat considerations, it becomes readily apparent that intelligence support to FP should be implemented robustly in Air Force processes, particularly threat assessments.

The threat drives everything accomplished in FP. *Identifying, understanding, and assessing the threat are the first steps in FP planning, followed by selecting the appropriate FP countermeasures.* **Threat assessments** for FP should be **systematic and continuous** to reduce uncertainties concerning the enemy and the battlespace for all types of operations. A force protection threat assessment analyzes and assesses the applicable area's land, sea, and aerospace dimensions. In addition to the typical threat-related areas, force protection threat assessments should include environmental, health, infrastructure, economic, political, and cultural aspects of the particular area of interest.

Force protection threat assessments should be all-source, fused analytical assessments. All-source should include using **national-level assets** (Defense Intelligence Agency [DIA]; National Security Agency [NSA];

Khobar Towers demonstrates the reality of the threat.

Federal Bureau of Investigation [FBI]; State Department Armed Forces Medical Intelligence Center [AFMIC]; Bureau of Intelligence and Research, Department of State [INR], etc.), **theater-level assets** (Joint Intelligence Center [JIC], Office of Special Investigations [OSI]), **in-country assets** (US Embassy, other in-country service components, etc.) and **local assets** (host-nation military, local law enforcement, etc.). Intelligence from these sources should be compiled, compared, evaluated, analyzed, and assessed by a threat assessment team comprised of available force protection personnel. The end product should provide commanders a baseline for conducting a **vulnerability assessment** and later for applying **the appropriate FP measures** for countering the threat. **Timely and accurate threat assessments are the key components in FP planning and operations.**

Once the threats are identified, the commander should employ a multifunctional vulnerability assessment team with expertise in the following areas: physical security; civil, electrical, and structural engineering; special operations; operational readiness; law enforcement and operations; infrastructure; weapons of mass destruction; health services; and intelligence/counterintelligence. In exceptional cases, commanders may tailor the team composition and the scope of the assessment to meet the unique requirements of a particular activity, however, commanders should meet the intent of providing a comprehensive assessment. The assessment team conducts an evaluation of the force to reveal the vulnerabilities and potential solutions relating to present and future threats.

Threat, Vulnerability, and Risk Assessments

Conducting threat, vulnerability, and risk assessments as parts to an overall risk assessment process permits commanders to identify potential threats and analyze vulnerabilities in order to determine the risks at a given location for a required mission. Chapter four discusses in detail these force protection tools available to commanders.

Countermeasures

At the heart of force protection doctrine is the need to counter the spectrum of threats against Air Force combat power when not directly engaged with the enemy. Countermeasures against one threat are often effective against a variety of similar or lesser threats. Chapter four discusses in detail force protection tools available to the commander to counter the threat.

Awareness

Force protection training is vital for Air Force personnel to survive and operate.

Commanders should ensure there is a fundamental emphasis on awareness of force protection challenges. *All personnel, regardless of rank or specialty, should be trained in basic force protection skills needed to survive and operate.* These should include basic weapons skills; basic ground combat skills; self-aid and buddy care; nuclear, biological, and chemical (NBC) defense; antiterrorism; field hygiene; threat awareness; safety awareness; and other essential common skills. Threat awareness training should include the full spectrum of threats and should emphasize that airmen understand all aspects of FP.

Awareness programs should raise the comprehension of Air Force personnel and their dependents of the general spectrum of threats and measures that will reduce personal vulnerability. Fundamental knowledge of the threats spectrum and measures to reduce personal vulnerability to threats should include:

- ✪ Spectrum of threat.
- ✪ Threat methods of attack and operations.
- ✪ Detecting surveillance by threat groups/agents.
- ✪ Individual protective measures.
- ✪ Hostage survival procedures.
- ✪ Threat levels and terrorist threat conditions (THREATCONs).
- ✪ Local threat updates.

Timely threat awareness updates are essential. Everyone, at all levels of command, needs to know about significant threat variations as soon as possible to implement force protection measures tailored to the

changing threat. Intelligence and effective on-site surveillance are the keys to timely threat awareness.

Command and Control

The command and control structure responds to threats and implements countermeasures against those threats. Commanders need intelligence on threat changes to make effective decisions to modify force protection postures and ensure personnel receive near-real-time awareness updates. A command and control structure should allow subordinate commanders to expedite requests for essential force protection resources and additional personnel from more senior command levels. For additional information, see the AFDD on Command and Control.

CHAPTER TWO

ORGANIZING FOR FORCE PROTECTION

…we can't be the best at building airplanes and submarines and second or third best at protecting our men and women.

General Shalikashvili, November 1996

COMMAND RESPONSIBILITY

Commanders at all levels have the responsibility for protecting Air Force assets. Command and control structures should enable commanders to rapidly and effectively address passive defense issues and quickly react to force protection threats with active defensive or offensive operations. Commanders are accountable for force protection within their areas. The unique nature of the force protection effort requires it be coordinated and integrated at the highest levels and across all functional areas. **Integrating all aspects of force protection into operations at all levels of command is one of the largest challenges of the commander.**

COMMAND RELATIONSHIPS

HQ USAF

The Chief of Staff, United States Air Force (CSAF), is responsible for providing guidance on how to organize, train, and equip forces. The CSAF exercises control over force protection programming, training, staffing, manning, and developing force protection policy. The Air Staff's primary function lies in allocating additional forces and funding as needed to fulfill force protection requirements.

Major Command (MAJCOM)

MAJCOM commanders are responsible for organizing, training, and equipping forces. MAJCOM commanders should integrate force protection requirements into every aspect of their activities. They should authorize cross-functional coordinating bodies to establish guidance, program for, and manage all force protection requirements for the MAJCOM, and to coordinate with the Air Staff.

Numbered Air Force (NAF)

The NAF should provide representation to the MAJCOM cross-functional staffs for force protection or provide inputs on requirements to their MAJCOM force protection focal point.

Air Force Forces (AFFOR)

A Commander, Air Force Forces (COMAFFOR), will serve as the commander of Air Force forces assigned or attached to a joint task force. A CINC-aligned NAF is typically redesignated as the AFFOR (e.g., 9 AF serves as US Central Command Air Forces [USCENTAF]). This organizational structure may be tailored by the COMAFFOR to fit specific mission needs. This staff does not exercise direct control but serves a planning, coordination, and oversight role. The organizational structure represented in figure 2.1 shows one example of how a COMAFFOR may organize the staff. **Centralized control of force protection resources and decentralized execution of force protection measures are essential to effectively protect our forces against each threat.**

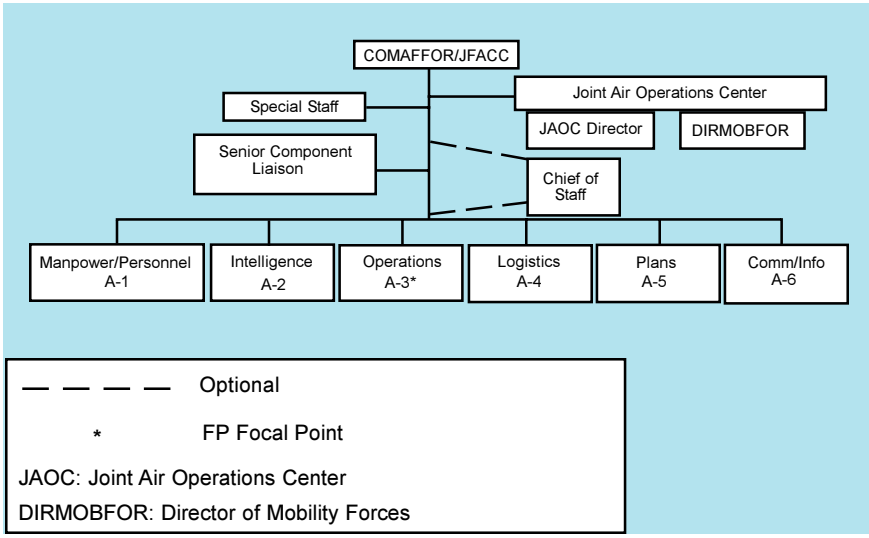

Figure 2.1. Headquarters Organization with COMAFFOR designated as the Joint Force Air Component Commander (JFACC)

Wing

Wing commanders face **three major force protection challenges: training** for force protection, **planning** for its integration and support as tasked in applicable operational plans, and **providing** force protection for assigned forces. Forward-based aerospace expeditionary wings (AEWs), similar to the standard AEW in figure 2.2, have the added responsibility of accomplishing force protection planning for the units identified to deploy to their location during contingency operations. Wing commanders should integrate force protection teams into their groups to establish guidance, program for, and manage force protection requirements for the wings. **Wing commanders should also appoint a single force protection focal point who should be an individual trained and knowledgeable in force protection issues; the Support Group commander has units with the resources to accomplish many force protection tasks and can serve in this capacity.**

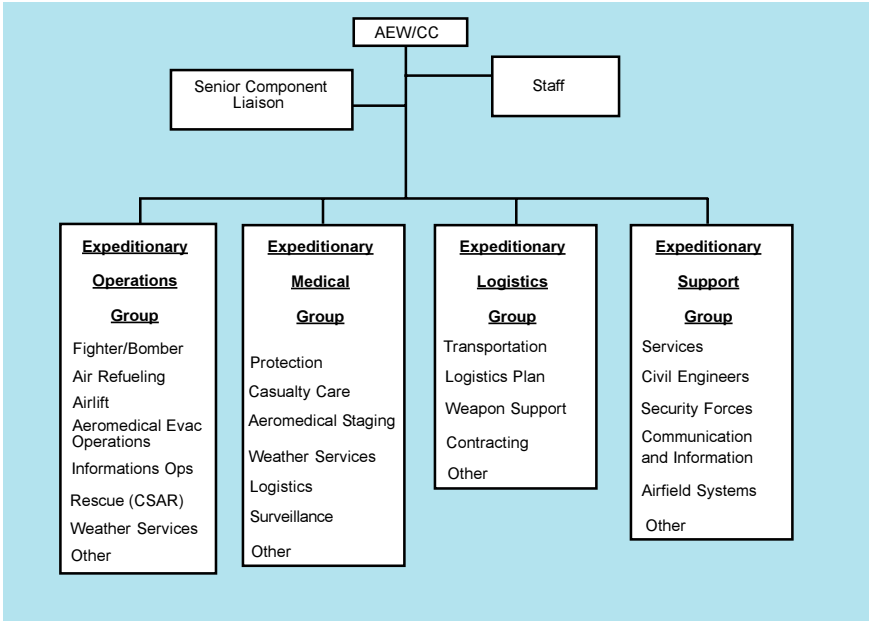

Figure 2.2. Standard Air Expeditionary Wing

CHAPTER THREE

FORCE PROTECTION THREATS

> ***Always presume that the enemy has dangerous designs and always be forehanded with the remedy. But do not let these calculations make you timid.***
>
> **Frederick the Great**

The essential goal of force protection doctrine is to describe the best way to counter threats against Air Force assets. Air Force personnel must identify the threats and determine ways to counter them before becoming directly engaged with the enemy.

FORCE PROTECTION THREAT SPECTRUM

The Air Force considers the following categories as serious threats that require force protection measures:

- **Conventional Threat**—Regular military forces supported by a recognized government are categorized as a conventional threat. Included in this threat are large tactical force operations including airborne, artillery, and missile attacks.

- **Unconventional Threat**—This threat encompasses a broad spectrum of military and paramilitary operations, normally of long duration, predominantly conducted by indigenous or surrogate forces who are organized, trained, equipped, supported, and directed in varying degrees by an

The Oklahoma City bombing is only one form of threat to force protection.

external source. It includes guerrilla warfare and other direct offensive, low visibility, covert, or clandestine operations, as well as the indirect activities of subversion, sabotage, intelligence activities, and evasion and escape networks.

- **Terrorism Threat—**This threat is a calculated use of violence or threat of violence to instill fear and intended to coerce or intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological.

- **Criminal Threat**—Criminal activity trends may help us predict future actions or even advanced warning of attack. Increased drug activity, unusual patterns of break-ins, bank robberies and stolen trucks could all indicate pending hostile action. Country, region, and international criminal activities with applicability to potential enemy actions or threat to friendly forces are the focus.

- **Insider Threat**—This threat comes from assigned personnel (military or civilian), host-country nationals (military or civilian), third country nationals (contract employees) or other persons assigned to or transiting the area of interest. Any of these groups of people may threaten Air Force assets primarily by disclosing sensitive or classified information, making decisions that favor dissident groups, and by attacking with weapons, explosives, biological agents, and computers. They may target individuals, groups, facilities, weapon systems, or information systems. The Air Force should assume this threat always exists and take appropriate precautionary measures.

- **Environmental Threat**—Air Force assets may be threatened by hazardous waste areas and hazardous materials production facilities. The threat also involves medical concerns such as disease, pestilence, and effects of the environment on individuals.

- **Weapons of Mass Destruction (WMD) Threat**—The WMD threat comes from systems that are capable of a high order of destruction or of being used to destroy large numbers of people. It can be nuclear, chemical, biological, and radiological weapons, but a WMD threat excludes the means of transporting or propelling the weapon where such means is a separable and divisible part of the weapon.

- **Civil Unrest Threat**—This threat reflects country-specific concerns of violence by the population related to friendly force operations. The threat can come from anti-American groups, protests, demonstrations, refugees, and humanitarian operations, and any local tensions that may escalate into a direct threat to our forces.

- **Information/Data Threat**—This threat results from attempts made by an enemy to achieve information superiority by affecting Air Force information, information-based processes, information systems, and computer-based networks while leveraging and defending their own information, information-based processes, information systems, and computer-based networks.

- **Future Threat**—New threats such as laser, microwave, acoustic weapons, or other high-technology weapons that adversaries may possess, have access to, or are developing should also be considered.

THREAT LEVELS

The categorized threats are grouped into four major threat levels: basic threats, level I threats, level II threats, and level III threats (see figure 3.1).

Threat Levels	Examples
Basic	Criminal, natural disasters, environmental, health, and disease threats, protestors, rioters,information resource threats
Level I	Agents, saboteurs, sympathizers, partisans, terrorists, extremist groups
Level II	Special purpose units, small tactical units, unconventional warfare forces, guerrillas
Level III	Large tactical forces, aircraft and/or theater missiles/ artillery with conventional or NBC weapons

Figure 3.1. Threat levels that force protection is designed to counter.

Basic Threats

Experience has shown that criminal activity, protests, riots, natural disasters, environmental, health, and disease threats, and attacks against information resources are basic threats that occur during peace and war. These threats can undermine mission capability as severely as sabotage or engagement with enemy forces as indicated in the bullets below.

- **Criminal:** Damaged or stolen government property and personal injury or death.

- **Natural disasters:** Damage or property losses, personal injuries or deaths due to severe thunderstorms, floods, tornadoes, hurricanes, ice storms, fires, and earthquakes.

- **Environmental and Health Threats:** Property and personnel losses, access or use denial due to fuel or chemical spills, pollution of resources, high incidence of disease in local population, and inadvertent or accidental release of toxins from hazardous materials production and destruction facilities.

- **Operational and Occupational Mishaps:** Personnel injuries and losses, and systems, facilities, and property damage and losses resulting from conditions other than natural disasters and intended losses or destruction.

- **Protestors, Rioters:** Physical damage, personal injury or death, and denial of access to resources.

- **Threats to Information Resources:** Unauthorized access, manipulation or destruction, hostile logic attack (for additional information, see the AFDD on Information Operations).

In addition to these basic threats, other threats have traditionally been divided into three more levels commonly accepted by all Services.

Level I Threats

Level I threats are characterized as small-scale operations conducted by agents, saboteurs, sympathizers, partisans, extremists, and agent-supervised or independently initiated terrorist activities. Level I threats

may be unorganized or well orchestrated and may take the form of espionage, demonstrations, riots, random sniper incidents, information warfare, physical assaults, kidnappings, aircraft hijackings, or bombings. This level of threat must be defeated by force protection measures.

Level II Threats

Level II threats include long-range reconnaissance, intelligence gathering, information warfare, and the sabotage of air or ground operations conducted by special-purpose, guerrilla, and unconventional forces or small tactical units. This level of threat must be defeated or delayed and mitigated by force protection measures until response forces arrive.

Level III Threats

Level III threats are major attacks by large tactical forces who may use airborne, heliborne, amphibious, and infiltration operations. Attacks may also come from aircraft and theater missiles/artillery armed with conventional and NBC weapons. This level of threat must be delayed and mitigated by force protection measures until the arrival of a tactical combat force (TCF). The US Air Force also uses its air warfare functions to counter and engage this threat; engagement of these forces in this manner takes it out of the realm of force protection.

It is easier and more effective to destroy the enemy's aerial power by destroying his nests and eggs on the ground than to hunt his flying birds in the air.

Giulio Douhet, 1921

THREAT METHODS OF ATTACK AND OBJECTIVES

Threats against Air Force assets are divided into the categories of methods of attack and the objectives those methods seek to accomplish.

Methods of Attack

✪ **Standoff Attacks—**These attacks are carried out from outside, sometimes far outside, a base perimeter.

✪✪ Standoff attacks were used in 75 percent of attacks since World War II.

Attacks by a small force with the limited objective of destroying aircraft have succeeded in destroying or damaging over 2,000 aircraft between 1940 and 1992. This fact is a powerful testimony to the effectiveness of small units using unsophisticated weapons against typical air base defenses and is a sobering precedent for those responsible for defending USAF bases against the threat.

Alan Vick,
Snakes in the Eagle's Nest

- ✪✪ Standoff attacks are difficult to counter.

✪ **Penetration Attacks—**A penetration attack is a form of offensive in which the enemy seeks to break through our defense and disrupt the defensive system.

- ✪✪ Penetration efforts were used in 22 percent of attacks since World War II.

- ✪✪ Penetration attacks were more prevalent in World War II and less in Vietnam.

✪ **Biological/Chemical Attacks—**Biological attacks use living organisms (naturally or artificially occurring) or their toxic by-products to produce casualties in personnel, animals, or plants and to contaminate food and water supplies. Chemical attacks employ chemical agents to kill, injure, or incapacitate personnel or animals for a significant period of time, and such attacks deny or hinder the use of areas, facilities, or material.

- ✪✪ Chemical and biological agents are possessed by many nations and nonstate actors.

- ✪✪ Information on development and use of biological and chemical agents is widely available.

- ✪✪ The FBI routinely conducts investigations into suspected use or plans to use biological or chemical agents. Bureau officials say a major attack in the US no longer seems unlikely.

✪ **Terrorist Attack—**Most recent threat trends involve the terrorist use of asymmetrical systems such as vehicle bombs against personnel, mov-

Chemical and biological weapons have been used throughout history in military combat. In 1710, during the war between Russia and Sweden, Russian troops used the cadavers of plague victims to create an epidemic. In 1767, during the French and Indian Wars, an English general surreptitiously provided the Indians loyal to the French with blankets infected with smallpox. In World War II, the Japanese used bubonic plague, cholera, anthrax, dysentery, typhoid, and paratyphoid in southeastern China. The Iraqi military used chemical weapons against both Iranians and Kurds in recent years. Chemical weapons were used by a terrorist group in a March 1995 attack on the Tokyo subway.

Multiple Sources

ing the focus away from the historically more common direct attacks against aircraft and their support infrastructure.

✪ **Objectives of Methods of Attack are to:**

✪✪ Injure or kill personnel to create a tactical and/or strategic event.

✪✪ Destroy war-fighting or war-supporting assets.

✪✪ Deny use of war-fighting or war-supporting assets through damage or contamination.

✪✪ Change ideology of governments.

✪✪ Force nations deployed on foreign soil to end operations and depart the deployed location.

✪✪ Thrust a nation into civil unrest resulting in civil war.

✪✪ Force a government agency or corporation to alter its environmental policies.

CHAPTER FOUR

COUNTERING THE THREATS

> ***…the Khobar Towers attack should be seen as a watershed event pointing the way to a radically new mindset and dramatic changes in the way we protect our forces….***
>
> **William J. Perry,**
> **Secretary of Defense,**
> **September 1996**

This chapter identifies a set of force protection tools for commanders to consider when preparing to counter threats in their areas. This begins with the risk assessment process and proceeds to force protection countermeasure planning and implementation.

RISK ASSESSMENT PROCESS

Commanders should begin by conducting a risk-based assessment. The process consists of identifying the potential threats and analyzing the vulnerabilities to determine the risks. Force protection working groups could manage this process for commanders.

Threat Assessment

A force protection threat assessment is the product of a threat analysis for a particular area. Force protection threat assessments fuse intelligence from human (HUMINT), signals (SIGINT), imagery (IMINT), and measurement and signature (MASINT) sources; counterintelligence; environmental; medical; information/data threat; and other information into a cohesive threat picture helpful to FP decision makers. Force protection threat assessments are conducted based upon specific criteria and the threat levels explained earlier in this document.

The threat analysis is a continual process of compiling and examining all available information concerning potential threats. A threat analysis will review the factors of a threat's existence, capability, intention, history, and targeting, as well as the security environment within which friendly forces operate. Threat analysis is an essential step in identifying the probability of attack and results in a threat assessment.

Vulnerability Assessment

Commanders should prepare a vulnerability assessment for facilities, installations, and operating areas within their area. The assessment will address the broad range of physical threats to the security of personnel and assets and it should be conducted periodically.

Vulnerability assessments for an area will normally be conducted by the installation commander. They should consider the range of identified and projected threats against a specific location or installation personnel, facilities, and other assets. They should evaluate the safety and vulnerability of local food and water sources, evaluate local medical capabilities, determine adequacy of hygiene of local billeting and public facilities, and perform an occupational and environmental risk evaluation. The assessments should identify vulnerabilities of Air Force assets, prioritized by their criticality to the mission, and propose solutions for enhanced protection.

Risk Assessment

Commanders should utilize threat and vulnerability assessments to make decisions about what level of risk they are willing to accept. Risks to the most critical Air Force assets should be eliminated whenever possible, but it is ultimately the commander's decision about what level of risk to accept.

Once the risk assessment is complete and all risk-level decisions made, commanders should use this information to plan a course of force protection actions to eliminate the risks they are not willing to accept and mitigate the risks they either cannot eliminate or have decided to accept.

FORCE PROTECTION COUNTERMEASURE PLANNING

Commanders should take deliberate action, once a risk assessment is made, to implement comprehensive force protection countermeasures to **deny an adversary information, access, and influence.** Commanders should exercise these measures to ensure their effectiveness. They can incorporate the following missions and tasks into their overall **defensive and offensive force protection** plan.

Deny Information

The Air Force denies an adversary information through a variety of **passive defense force protection measures.** Protecting sensitive information is the key to force protection countermeasure planning. Denying potential adversaries the intelligence necessary to plan and conduct hostile actions is the most effective but also the most difficult means to enhance force protection. The following capabilities exist to assist commanders in executing FP responsibilities:

- **Counterespionage Programs—** These are activities conducted to detect, deter, and neutralize adversary intelligence gathering. They consist of interdisciplinary measures combining personnel security, awareness, and reporting that prompt investigations to neutralize a threat. These programs also consist of independent offensive operations to engage adversarial HUMINT capabilities to deny the adversary's intelligence objectives or influence the adversary's understanding of the environment.

- **Technical Security Countermeasure Surveys—** These surveys are the means by which adversary technical intelligence gathering capabilities are detected and neutralized. They contain interdisciplinary evaluations of physical security, access control, technical security and the identification of vulnerabilities specific to those disciplines. The surveys also identify clandestine technical intelligence collection means to be neutralized or exploited.

- **Operations and Information Security Vulnerability Assessments—** These assessments identify vulnerabilities associated with operations security (OPSEC) and information security (INFOSEC) to include evaluations of sensitive, but unclassified, intelligence information available to an adversary. The assessments should disclose vulnerabilities of friendly personnel to adversarial intelligence gathering methods. These assessments could be useful in raising personnel security awareness and aid in lowering the observable profile of aerospace operations.

- **Information Security and Information Assurance—** Information security provides guidance for classification, protection, and dissemination of classified national security information processed within any information system. Information assurance provides measures to pro-

tect friendly information systems by preserving the availability, integrity, and confidentiality of the systems and the information contained within the systems. Air Force communications and information resources are force multipliers that support the current core competencies of the Air Force: air and space superiority, global attack, rapid global mobility, precision engagement, information superiority, and agile combat support. The communications and information infrastructure is undergoing significant mission and technology-driven changes to ensure information is delivered at the right time and place, anywhere on the globe. These changes demand an integrated information protection approach that embraces the war-fighter's mission and ensures operations are done securely. Measures are being implemented to ensure our information resources are adequately protected. Every commander and information system user should ensure these measures are used correctly and fully. More guidance can be obtained in the AFDD on Information Operations.

✪ **Camouflage, Concealment, Deception (CCD)**—CCD is the capability to reduce the effectiveness of attacking forces and reconnaissance assets through the principles of hide, blend, disguise, and decoy to protect friendly assets and aim points with materials and equipment that alter or obscure part or all of their multispectral signatures.

Camouflage.

✪✪ **Hide.** To conceal an asset from visual or sensor aided acquisition.

✪✪ **Blend.** To combine the parts of a scene or target so as to render the parts indistinguishable.

✪✪ **Disguise.** To modify so as to prevent recognition of the true identity or character of an asset or activity.

✪✪ **Decoy.** To simulate an object or use a signature generator to simulate a potential target.

Deny Access

The Air Force denies access to adversaries through the application of **defensive and offensive force protection measures.** Integrated with measures that deny information to an adversary are measures to deny access if an enemy attempts to collect available intelligence. The objective of denying access is to prevent or deter a hostile action by limiting vulnerabilities of personnel and operations.

Measures to Deny Access

✪ **Surveillance Detection and Countersurveillance—**Technical and human sources of information identify potentially hostile surveillance to evaluate it as a threat and implement countermeasures. Countermeasures may include relocating targeted assets; increased security posture; and cover or concealment. Countersurveillance operations may also be executed offensively to identify suspected surveillance and disrupt potentially hostile intelligence gathering methods.

✪ **Protective Service Operations—**Personal protective operations are undertaken on behalf of a high risk or key individual to reduce the risk of assassination, kidnapping, or other physical harm.

✪ **Protective Threat Assessments and Vulnerability Surveys—**Time, location, and threat-specific evaluations of potential individual targets should be conducted for the identification of particular vulnerabilities. These assessments and surveys help meet a short-term need to increase the security posture of the facility evaluated or person being protected.

Air Force Assets

The Air Force routinely categorizes assets as **priority resources** (mission-essential aircraft, weapon systems, and command, control, and communications, space, and intelligence resources) and **nonpriority resources** (other high value Air Force assets such as ground vehicles, petroleum storage sites, nonoperational transport aircraft, etc.).

Physical security provides deterrence.

✪ **Priority Resources—Physical security** is a tightly focused security capability that deters and responds to hostile operations against **priority** Air Force resources. Physical security achieves the appropriate degree of deterrence and is effective through designing and fielding security systems that:

- ✪✪ **Control entry and access** to sensitive areas with priority assets;
- ✪✪ **Detect** hostile activity against priority assets; and
- ✪✪ If necessary, **defeat a hostile force** targeting priority assets.

✪ **Nonpriority Resources—Resource protection** is a broad-based security capability for protecting **nonpriority** Air Force resources through four objectives:

- ✪✪ Maintain the Air Force warfighting capability by **reducing damage to nonpriority Air Force resources.**
- ✪✪ Safeguard Air Force property by **reducing the opportunity for theft or attack by making a potential nonpriority target inaccessible or unattractive.**
- ✪✪ Use Crime Prevention Through Environmental Design (CPTED) principles that focus on **preventing resource loss through facility and environmental planning.** CPTED examples include better use of lighting and architectural designs that emphasize ease of surveillance by friendly forces.

✪✪ Ensure **everyone safeguards government property.**

Combatting Terrorism

Combatting terrorism is actions taken to protect Air Force personnel and property from terrorist acts and to oppose terrorism in all forms. Combatting terrorism includes antiterrorism (defensive measures taken to reduce vulnerability to terrorist acts) and counterterrorism (offensive measures taken to prevent, deter, and respond to terrorism). Actions may include implementation of random measures to protect Air Force populace from terrorist activities, installation of physical security aids, and education and awareness training.

Antiterrorism measures can reduce vulnerability to terrorist acts.

Air Base Defense

Air base defense generally describes actions taken by force protection forces in theater preparing for an overt attack by level I, II, or III threats.

- ✪ Forces should be organized to **prevent and defeat attacks.**
- ✪ Forces should be **integrated into rear security operations** with other Services, host-nation and allied or coalition forces.
- ✪ The senior Air Force commander respon-

Air base defense preparation for an overt attack.

sible for each air base may delegate authority to conduct air base defense to a **subordinate commander.**

Deny Influence

The Air Force denies adversarial influence through *force health protection, disaster preparation, and ability to survive and operate (ATSO) actions.*

Force health protection denies influence by:

- ✪ Promoting **fitness** for enhanced performance at all times, including before and during deployments.
- ✪ Assuring **healthy and safe food and water.**
- ✪ Providing **mission-tailored casualty care capability.**
- ✪ **Preventing or controlling infectious diseases** including those from **biological agents.**
- ✪ Ensuring awareness of **environmental and occupational threats.**

Force health protection is vital to a fit and ready force.

- **Protecting** personnel from **hazardous materials** including **chemical agents.**

- **Preventing injuries** from combat action, mishaps, and recreation.

- **Conducting medical surveillance** and information.

For additional information, see the AFDD on Health Services.

Disaster preparation is the capability to deny influence by enhancing force survivability and mission continuation through:

- **Dispersal, sheltering, evacuation, or relocation** of materiel and people needed for mission accomplishment and recovery tasks.

- Use of **individual protective equipment.**

- **Mutual support agreements** with civilian authorities, local US and DOD agencies, and host nation.

Disaster preparation enhances force survivability and mission continuation.

- **NBC contamination control, warning, plotting, predicting, and reporting.**

- **Mitigating** the **effects** of and **enhancing recovery** from major accidents and natural disasters.

Ability to survive and operate (ATSO) denies influence through the ability to preserve, sustain, or restore a force's mission capability before, during, and after an enemy attack. Capabilities should include:

- **Attack detection** and **warning.**

- **Reconnaissance** after attack.

- **NBC contamination avoidance.**

- **Damage repair,** fire protection, and individual protection.

- **Structural engineering, hardening, and infrastructure engineering** to increase structural strength and ballistic protection.

- **Explosive ordnance disposal to protect personnel and resources from unexploded ordnance.**

> ***Static aircraft protection embarked on a new phase in 1968 as the Air Force launched a crash shelter construction program.…The protection afforded aircraft by hardened shelters confirmed the soundness of the program.…Seventh Air Force on 3 June 1969 cited two cases in which aircraft parked in shelters escaped destruction by direct rocket hits. On another occasion shelters saved several aircraft from damage or destruction when a nearby munitions storage area exploded. In spring 1970 a USN EC-121 crashed and burned at Da Nang, but adjacent hardened shelters saved three USAF F-4Ds from destruction and two others from major damage. The estimated dollar savings attributed to shelters in these incidents more than paid for the $15.7 million program in [the Republic of Vietnam].***
>
> **Roger P. Fox,**
> ***Air Base Defense in the Republic of Vietnam: 1961-1973***

In summary, the comprehensive measures outlined above are tasks and objectives historically proven to be effective in providing force protection *when properly implemented.* Recent trends in the development of aerospace expeditionary forces could lead to tasks and objectives not conducted in past operations.

CHAPTER FIVE

FORCE PROTECTION TRENDS

Security no longer ends at the base perimeter. We must assume responsibility for a much larger tactical perimeter that will keep the threat away from our people and equipment.

General Ronald R. Fogleman, 1997

Since the end of the Cold War, the US Air Force has made great strides toward becoming an expeditionary aerospace force. Since 1986, the Air Force has downsized by 36 percent while overseas contingencies have greatly increased. In 1989, the Air Force averaged 3,400 people deployed for contingencies and exercises. Since the end of DESERT STORM, the average had grown to 14,600 in FY 97. Many deployments, due to short time constraints and/or austere conditions, cannot expect external (US Army, host nation, or coalition) force protection forces to be available. These contingencies and AEF **deployments require** the Air Force to go forward with **an organic force protection capability.**

Protecting the force is everyone's duty. Force protection should be a basic military skill taught to all Air Force members. Security forces (SF) should not hold sole responsibility for defending the force. Marines and soldiers are trained as infantry first, regardless of their military specialty. In the Navy all sailors are trained in fire and damage control. Decreases in Air Force manpower and increases in operational demands mandate that everyone in the Air Force assume a greater force protection role. Everyone has a role either in generating or sustaining aerospace power under all conditions and protecting the force at all times.

[In 1964] General LeMay…revealing he knew the token character of the USAF general military training program…ordered that "the means each individual has for self-protection and weapons qualification" be given special attention.

Roger P. Fox,
Air Base Defense in the Republic of Vietnam: 1961-1973

Every Air Force installation, base, or deploying organization requires organic force protection assets. Commanders field all required force protection assets based on a risk assessment of force vulnerability, which will also be accomplished at the home station so as to not be compromised when that unit is deployed.

Advancements in technology can provide force enhancement but not always force replacement. This is a critical distinction. For example, sensors and imaging devices release force protection personnel from static posts and allow them increased mobility and flexibility. Technology can assist force protection, yet may still require the person to accomplish the mission.

Force protection resource allocations are risk based and programmatically sustained. Force protection is a long-term investment program. In the past, the United States has increased force protection investments only after something devastating has happened. A cyclical pattern has not worked in the past and it will not work to protect Air Force assets in the future. Past oversights and shortcomings must be changed through a sustained effort. History has demonstrated that only when an adequate force protection infrastructure is in place should an Air Force system be fielded.

Force protection is critical to mission success.

Force protection resources, including manpower, are properly borne by the system program and are part of the acquisition program baseline. This is increasingly important as we close installations and maintain the strategy of forward presence required by global engagement.

At the Very Heart of Warfare lies Doctrine . . .

Suggested Readings

Air Force Doctrine Document 2-4.2, *Health Services.*

Air Force Doctrine Document 2-5, *Information Operations.*

Air Force Doctrine Document 2-8, *Command and Control.*

Joint Publication 3-07, *Joint Doctrine for Military Operations Other Than War.*

Joint Publication 3-07.2, *Joint Tactics, Techniques, and Procedures for Anti-terrorism.*

Joint Publication 3-10, *Joint Doctrine for Rear Area Operations.*

Joint Publication 3-10.1, *Joint Tactics, Techniques, and Procedures for Base Defense.*

Joint Publication 3-11, *Joint Doctrine for NBC Defense.*

Joint Publication 3-13, *Joint Doctrine for Information Operations.*

Roger P. Fox, *Air Base Defense in the Republic of Vietnam: 1961-1973,* (USAF Office of History), 1979.

Keith William Nolan, *The Battle for Saigon—Tet 1968,* (Pocket Books), 1996.

David A. Shlapak & Alan Vick, *Check Six begins on the ground*, (RAND), 1995.

Alan Vick, *Snakes in the Eagle's Nest,* (RAND), 1995.

Glossary

Abbreviations and Acronyms

AEF	aerospace expeditionary force
AEW	Aerospace Expeditionary Wing
AFDD	Air Force doctrine document
AFFOR	Air Force forces
AFMIC	Armed Forces Medical Intelligence Center
AFP	Active Force Protection
AOR	area of responsibility
ATSO	ability to survive and operate
CCD	camouflage, concealment, deception
CINC	commander in chief
COMAFFOR	Commander, Air Force Forces
CPTED	Crime Prevention Through Environmental Design
CSAF	Chief of Staff, US Air Force
CSAR	combat search and rescue
DIA	Defense Intelligence Agency
DIRMOBFOR	Director of Mobility Forces
DOD	Department of Defense
FBI	Federal Bureau of Investigation
FP	force protection
HUMINT	human intelligence
IMINT	imagery intelligence
INFOSEC	information security
INR	Bureau of Intelligence and Research, Department of State
JAOC	joint air operations center
JFACC	joint force air component commander
JP	joint publication
MAJCOM	major air command
MASINT	measurement and signature intelligence
NAF	numbered air force

NBC	nuclear, biological, chemical
NSA	National Security Agency
OFP	Offensive Force Protection
OPSEC	operations security
OSI	Office of Special Investigations
PFP	Passive Force Protection
SF	security forces
SIGINT	signals intelligence
TCF	tactical combat force
THREATCON	terrorist threat conditions
USCENTAF	US Central Command Air Forces
WMD	weapons of mass destruction

Definitions

active force protection. Measures to defend against or counter a perceived or actual threat and, if necessary, to deny, defeat, or destroy hostile forces in the act of targeting Air Force assets.

area of responsibility. The geographical area associated with a combatant command within which a combatant commander has authority to plan and conduct operations. Also called **AOR.** (JP 1-02)

combatting terrorism. Actions, including antiterrorism (defensive measures taken to reduce vulnerability to terrorist acts) and counterterrorism (offensive measures taken to prevent, deter, and respond to terrorism), taken to oppose terrorism throughout the entire threat spectrum. (JP 1-02)

force health protection. A comprehensive threat-based program directed at preventing and managing health-related actions against Air Force uncommitted combat power.

force protection. Security program designed to protect Service members, civilian employees, family members, facilities, and equipment, in all locations and situations, accomplished through planned and integrated

application of combatting terrorism, physical security, operations security, personal protective services and supported by intelligence, counterintelligence, and other security programs. (JP 1-02) Because terminology is always evolving, the Air Force believes a more precise definition is: [*Measures taken to prevent or mitigate successful hostile actions against Air Force people and resources while not directly engaged with the enemy.*] {Italicized definition in brackets applies only to the Air Force and is offered for clarity.}

information operations. Actions taken to affect adversary information and information systems while defending one's own information and information systems. Also called **IO.** (JP 1-02) Because terminology is always evolving, the Air Force believes a better definition of information operations is: [*Those actions taken to gain, exploit, defend, or attack information and information systems. This includes both information in warfare (IIW) and information warfare (IW).*] {Italicized definition in brackets applies only to the Air Force and is offered for clarity.}

offensive force protection. Proactive measures taken to deny, defeat, or destroy hostile forces who currently are not committed to direct hostile activity but whose intent is to target Air Force assets not currently engaged in combat operations.

passive force protection. Measures to negate or reduce the effects of hostile acts on Air Force assets by making them more survivable. This can be proactively accomplished through training, education, hardening, camouflage, concealment, deception, information security, and low/zero observable execution.

tactical combat force. A combat unit, with appropriate combat support and combat service support assets, that is assigned the mission of defeating Level III threats.(JP 1-02)